Multifactor Authentication User Guide

Prepared for:

Wyoming Department of Health
122 West 25th Street, 4 West
Cheyenne, WY 82002

Prepared By:

CNSI
2277 Research Boulevard
Rockville, MD 20850

October 25, 2021
Version 1.0
Security: N = No Restriction

Table of Contents

Figures

Tables

Purpose and Scope

Wyoming Medicaid is a federal and state program that provides health and Long Term Care (LTC) coverage to low-income children, parents, seniors, and people with disabilities living in Wyoming. You can find Information about the Wyoming Medicaid program at https://www.wyomingmedicaid.com/.

You'll find a **Providers** quick access link on the Wyoming Medicaid Home page. It gives you access to both information related to Medicaid service providers and the secure Provider Portal. After registering with Wyoming Medicaid, you can sign into the secure Provider Portal and view information about your provider account and perform various actions, such as enrolling a Billing Provider/Clearing House.

Wyoming Medicaid provides the option to sign into your application(s) on the secure Provider Portal using a Single Sign On (SSO) username and password. During the registration process outlined in the Provider SSO Registration User Guide, you'll need to register a method for multifactor authentication.

There are three (3) total options. They are as follows:

- Okta Verify
- Google Authenticator
- SMS Verification

This guide walks you through the process of setting up each one of those options. You may choose one or more of the options for multifactor authentication. However, the only option available to use on a personal computer (PC) or Windows-based laptop is Google Authenticator. All the options work on a smart phone. The SMS Verification method works on any device capable of receiving text messages.

For a full walkthrough of the registration process, please refer to the *Provider Single Sign On Registration User Guide*.

Browser Compatibility

The security features of the Wyoming Medicaid website require that you use one of the following web browser versions or later:

- Google Chrome Version 90.0.4430.212 (64-bit)
- Firefox Version 88.0.1
- Microsoft Edge Version 90.0.818.62 (64-bit)

Document Conventions

This document uses the following conventions:

- The terms "you" and "user" in this document refer to the Provider Administrator who registers the provider account for access to the secure Provider Portal.

- An **Important Note**, presented in the following style:

	Provides important information the user needs to observe or act upon.

Chapter 1 – Multifactor Authentication Page

For both new users and returning users who have not used multifactor authentication, the **Multifactor Authentication Page** displays.

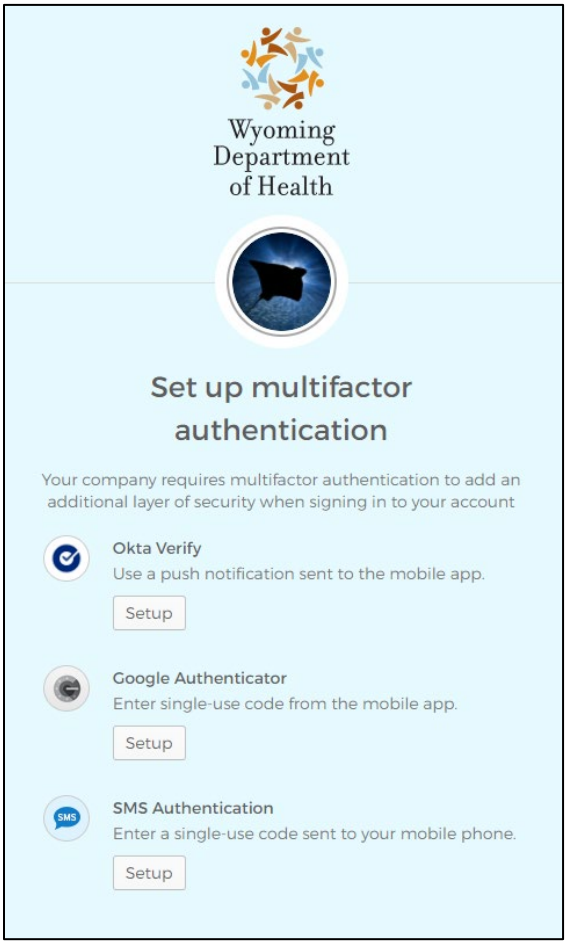
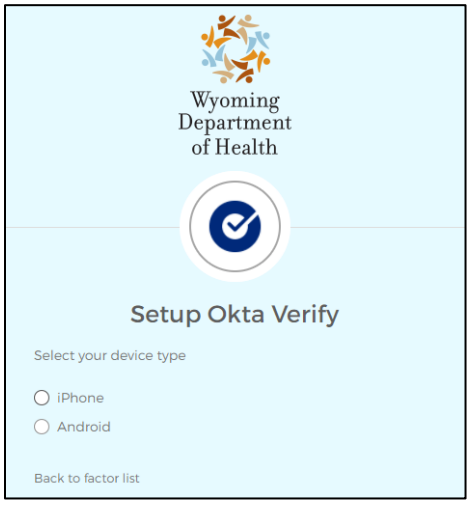


Figure 1. Multifactor Authentication Page

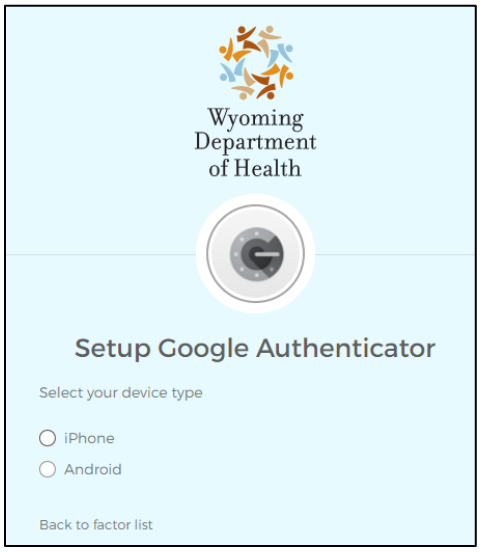
> **For authentication using a PC, you'll need to set up the Google Authenticator.** Refer to Chapter 3 – Google Authenticator Setup for detailed instructions on how to complete any or all of these three MFA choices. You can find those instructions on the Tutorials page and on the Provider Homepage in the same location as this document.

1. Choose a multifactor authentication method and follow the on-screen instructions. You can choose from **Okta Verify**, **Google Authenticator**, or **SMS Authentication**. You can set up more than one verification, but only the Google Authenticator works on a personal computer (PC).

- **Okta Verify:** Requires a smart phone app for use.



- **Google Authenticator:** Smart phone or on a PC using the Chrome browser.



- **SMS Authentication:** Requires a phone or device that can receive text messages.

2. Select the radio button next to the system of your choice.
3. Select **Setup.**
4. Follow the onscreen instructions or follow the corresponding section in this document.

You can set up one or more MFA methods. After setting up one method, this multifactor authentication page displays with two sections showing enrolled factors and additional optional factors as displayed in Figure 2.

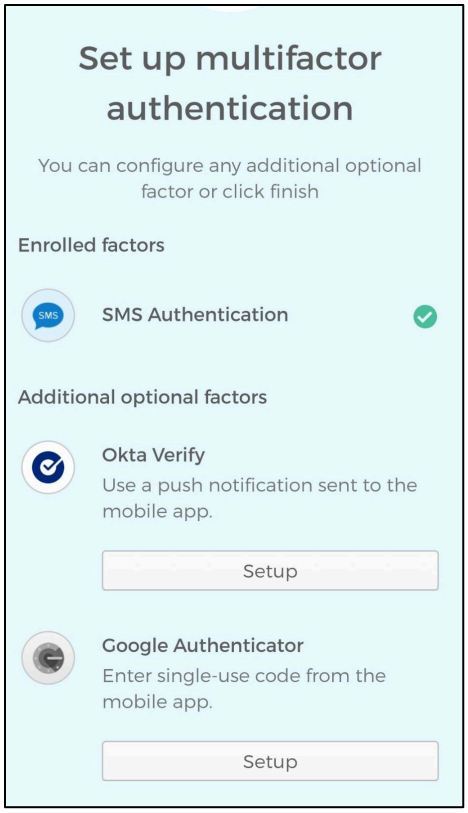


Figure 2.Additional Multifactor Authentication Setup

1. Select the **Setup** button next to your additional choice.
2. Follow the instructions in the corresponding section of this document or the on-screen instructions.
3. Select **Finish** when you are done setting up your additional method(s).

Chapter 2 – Okta Verify Setup

After choosing the Okta Verify setup from the Multifactor Authentication page shown in Figure 1, the following page displays:

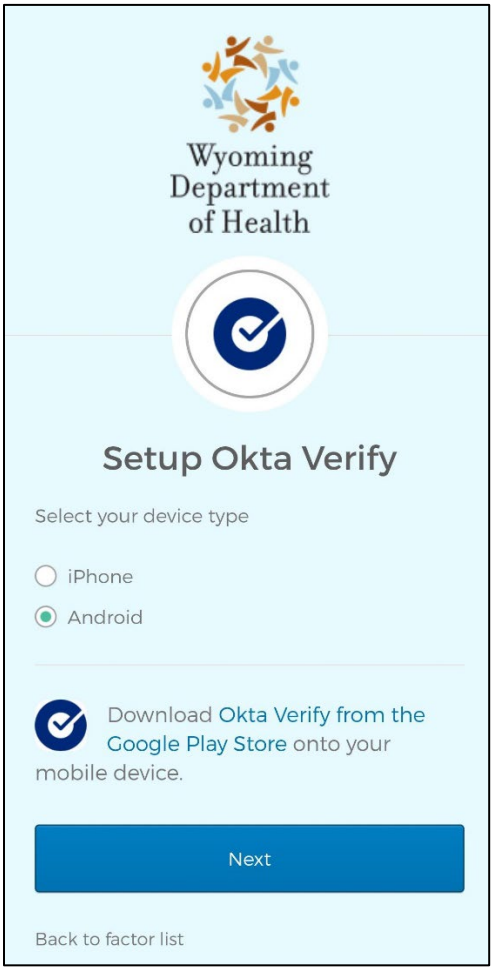


Figure 3. Okta Verify Setup Page

Once you've selected iPhone or Android from the device type list, a link to the appropriate store displays.

1. Select the link or navigate to the Apple store for iOS systems (iPad and iPhone) or the Google Play store for Android systems on your device.
2. Download and install the "**Okta Verify**" app.
3. Select **Next**.
4. A QR code displays with the instructions "Launch Okta Verify application on your mobile device and select Add an account."

6. Select the "**+**" sign at the top to add an account.
7. You can then scan the QR code. If you are unable to scan the QR code:
    a. Select the **Can't Scan** link below the barcode. Then finish Okta Verify setup using an SMS (text) message, manual setup, or email following the on-screen instructions.
    b. Select your preferred method from the dropdown list.
        - **For SMS:**
            i. Select the country from the dropdown list and enter your phone number.
            ii. Then select the login link sent to you via text message.
        - **For Email:**
            i. select email from the dropdown list and select **Send**.
            ii. Select the link sent to the email address you registered with the system.
        - **For Setup without Push Notifications:**
            i. Select setup manually without push notifications.
            ii. Copy the Secret Key.
            iii. Select **Next**.
            iv. Enter your username and then the Secret Key you copied into the Secret Key field.

Chapter 3 – Google Authenticator Setup and Use

The Google Authenticator app can be used on an Android, iPhone, or Blackberry device. To use Google Authenticator on your Android device, it must be running Android version 4.4 or later. To use Google Authenticator on your iPhone, iPod Touch, or iPad device, you must have iOS5. With 2-Step Verification (also known as two-factor authentication), you add an extra layer of security to your account in case your password is stolen. After you set up 2-Step Verification, you'll sign into your account in two steps using:

- Something you know, like your password
- Something you have, like your phone or computer.

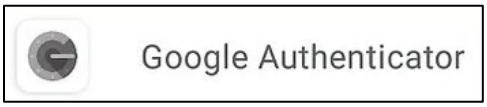
If you are a clearinghouse or billing agent, it is strongly recommended you set up your Google Authenticator using your computer. If you are a pay-to-provider (except for Waiver providers) it is strongly recommended you set up your Google Authenticator using your computer. Using a cellphone for the Google Authenticator will require access to that cell phone every time the Multi-Factor Authentication (MFA) is required. If you do not have access to that device at the time you need to access your SSO, it is recommended that you complete the Google Authenticator using your computer.

3.1 Phone or Mobile Device Installation

3.1.1 Android Device

To use Google Authenticator on your Android device, you need Android version 4.4 and up.

1. Open the Play Store on your Android device (it's the multicolored triangle icon labeled "Play Store" in your app list).
2. Type 'Google Authenticator' into the Search Bar (it's located at the top of the play store).
3. Tap 'Google Authenticator' in the search results (it's the app result with the grey vault icon).



4. Tap the green 'Install' button. Depending on your settings you may have to verify your PIN or approve the download. When the download is complete, the 'Install' button changes to read 'Open', and the authenticators vault icon is added to your device's app list.
5. Open Authenticator. If you're still in the 'Play Store' tap 'Open'. Otherwise, tap the new vault icon in your app list.
6. Tap 'Get Started'. This takes you to the 'Setup your first account' screen.

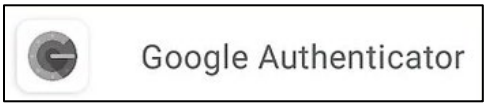
7. This screen provides you the option to scan a QR code or enter a setup key. When you are prompted to link the Google Authenticator with your SSO, this is the screen of your Google Authenticator this is completed on. Be prepared to scan the generated QR code.

> Please note that you can use Google Authenticator to sign into many different sites and services, including Google, Facebook, Amazon, and more. If you are using your personal cellphone device, please keep that in mind, as you will need to ensure you are using the correct google chrome account to use the authenticator for OKTA access.

3.1.2 iOS Operating Systems (Mac, iPhone, and iPad)

To use Google Authenticator on your iPhone or iPad device, you need iOS5 and up. You'll use this same method for a Mac.

1. Open the App Store on your Mac, iPhone, or iPad (it's the blue icon with a white 'A' in your app list).  .
2. Tap 'Search' (it's the magnifying glass at the bottom-right corner).
3. Type 'Google Authenticator' into the Search Bar and tap 'Search'. This displays a list of matching search results.
4. Tap 'Google Authenticator' in the search results (it's the app result with the grey vault icon).



6. Open the Authenticator. If you're still in the App Store, tap 'Open'. Otherwise, tap the new vault icon on your home screen.
7. Tap 'Get Started'. This takes you to the 'Setup your first account' screen.
8. This screen provides you the option to scan a QR code or enter a setup key. When you are prompted to link the Google Authenticator with your SSO, this is the screen your Google Authenticator is completed on. Be prepared to scan the generated QR code.

> Please note that you can use Google Authenticator to sign into many different sites and services, including Google, Facebook, Amazon, and more. If you are using your personal cellphone device, please keep that in mind that you need to ensure you are using the correct google chrome account to use the authenticator for OKTA access.

3.2 Windows Based Personal Computer (PC) Installation

In Chrome, go to the web store: https://chrome.google.com/webstore/category/extensions

1. Type 'Google Authenticator' in the search field located at the top left of the screen.
2. Next to Authenticator, click Add to Chrome. You have now successfully added the extension.

3.3 How to use Google Authenticator

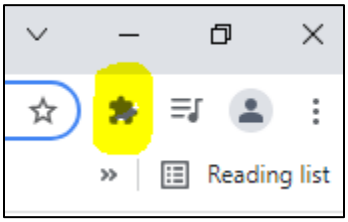
3.3.1 Smartphone or Pad

If you elected to use your smart phone, iPhone or Pad device to complete your google authentication, you will need to scan the QR code that generates after you log into the system using SSO.

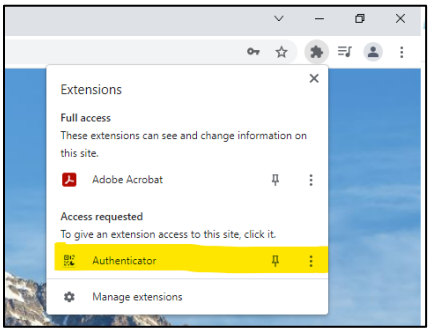
3.3.2 Computer

If you elected to use your computer and have installed the Google Authenticator extension to your Google Chrome browser, then proceed with logging into your SSO account. When prompted, indicate that you are using an android cell phone device, and then a scannable QR code appears on the screen.

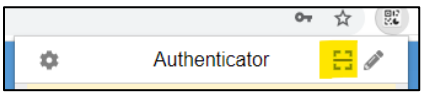
1. Open the 'puzzle piece' to access your Google Chrome extensions:



2. Select 'Google Authenticator' from the dropdown menu.



3. Select the QR Scan Icon:



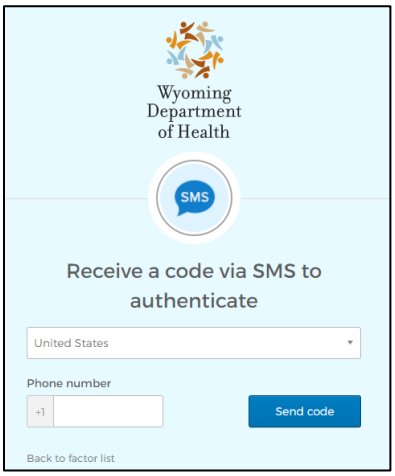
4. Select (click) and drag around the generated QR code, and the account is added to the Google Authenticator.

5. Then you can generate an MFA code using Google Authenticator, which links to your SSO login. Use this MFA process every time you log into your SSO account.

Chapter 4 – SMS Authenticator Setup

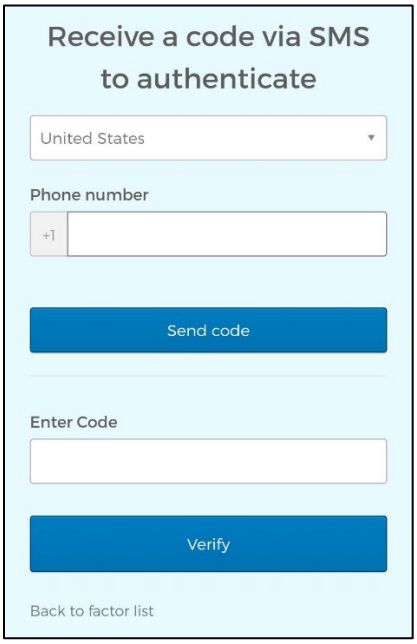
SMS Authenticator setup uses any device with a phone number capable of receiving text messages. Typically, you'll use a cell phone for this method.

1. Once you choose the SMS Authenticator method from the screen displayed in Figure 1. Multifactor Authentication Page, the **Receive a code via SMS to authenticate screen** appears.



2. Choose the country your phone number is based in from the dropdown list. The default is the United States.
3. Enter your phone number into the **Phone Number** field.
4. Select the **Send Code** button.

   The **Enter Code** field displays.



5. Enter the code you received via SMS (text message) in the **Enter Code** Field. If you did not receive a code, select the **Resend Code** Option.

Appendix A – Acronyms

Table 1. Acronyms

Page Element	Description
EIN	Employer Identification Number
SSN	Social Security Number
SSO	Single Sign-On
MFA	Multifactor Authentication
SMS	Short Message Service (commonly called "text message")
QR [Code]	Quick Response [Code]